

An extended characterization of a class of optimal three-weight cyclic codes over any finite field

Gerardo Vega

Abstract

A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field was recently presented in [10]. Shortly after this, a generalization for the sufficient numerical conditions of such characterization was given in [3]. The main purpose of this work is to show that the numerical conditions found in [3], are also necessary. As we will see later, an interesting feature of the present work, in clear contrast with these two preceding works, is that we use some new and non-conventional methods in order to achieve our goals. In fact, through these non-conventional methods, we not only were able to extend the characterization in [10], but also present a less complex proof of such extended characterization, which avoids the use of some of the sophisticated –but at the same time complex– theorems, that are the key arguments of the proofs given in [10] and [3]. Furthermore, we also find the parameters for the dual code of any cyclic code in our extended characterization class. In fact, after the analysis of some examples, it seems that such dual codes always have the same parameters as the best known linear codes.

Keywords: Cyclic codes, weight distribution, exponential sums, Griesmer lower bound.

I. INTRODUCTION

In coding theory an interesting but at the same time a difficult problem is to determine the weight distribution of a given code. The weight distribution is important because it plays a significant role in determining the capabilities of error detection and correction of a code. For cyclic codes this problem is even more important because this kind of codes possess a rich algebraic structure. On the other hand, it is known that cyclic codes with few weights have a great practical importance in coding theory and cryptography, and this is so because they are useful in the design of frequency hopping sequences and in the development of secret sharing schemes. A characterization of a class of optimal three-weight cyclic codes of dimension 3, over any finite field, was recently presented in [10], and almost immediately after this, a generalization for the sufficient numerical conditions of such characterization was given in [3]. By means of this generalization it was found a class of optimal three-weight cyclic codes of dimension greater than or equal to 3 that includes the class of cyclic codes characterized in [10].

The main purpose of this work is to show that the numerical conditions that were found in [3] are also necessary. As we will see later, an interesting feature of the present work is that, in clear contrast with [10] and [3], we use some new and non-conventional methods in order to achieve our goals. More specifically, we will use the remainder operator (see next section for a formal definition of it) as one of the key tools of this work. In fact, through this remainder operator, we not only were able to extend the characterization in [10], but also present a less complex proof for such extended characterization, which avoids the use of some of the sophisticated –but at the same time complex– theorems (for example the Davenport-Hasse Theorem), that are the key arguments of the proofs given in [10] and [3]. As a consequence, we were also able to present a simplified and self-contained proof of our extended characterization. As a further result, we also find the parameters for the dual code of any cyclic code in our extended characterization class. In fact, after the analysis of some examples, it seems that such dual codes always have the same parameters as the best known linear codes.

G. Vega is with the Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, 04510 Ciudad de México, MEXICO (e-mail: gerardov@unam.mx).

Manuscript partially supported by PAPIIT-UNAM IN107515.

In order to provide a detailed explanation of what are the main results of this work, let q and k be positive integers such that q is a power of a prime number, and fix $\Delta = \frac{q^k-1}{q-1}$. Also let γ be a fixed primitive element of \mathbb{F}_{q^k} . For any integer a , denote by $h_a(x) \in \mathbb{F}_q[x]$ the minimal polynomial of γ^{-a} . With this notation in mind, the following result gives a full description for the weight distribution of a class of optimal three-weight cyclic codes of length $q^k - 1$ and dimension greater than or equal to 3.

TABLE I
Weight distribution of $\mathcal{C}_{(\Delta e_1, e_2)}$.

Weight	Frequency
0	1
$q^{k-1}(q-1)-1$	$(q-1)(q^k-1)$
$q^{k-1}(q-1)$	q^k-1
q^k-1	$q-1$

Theorem 1: Suppose $k > 1$, and for any two integers e_1 and e_2 , let $\mathcal{C}_{(\Delta e_1, e_2)}$ be the cyclic code, over \mathbb{F}_q , with parity-check polynomial $h_{\Delta e_1}(x)h_{e_2}(x)$. If $\gcd(q-1, ke_1 - e_2) = 1$ and $\gcd(\Delta, e_2) = 1$ then

- (A) $\deg(h_{\Delta e_1}(x)) = 1$ and $\deg(h_{e_2}(x)) = k$. In addition, $h_{\Delta e_1}(x)$ and $h_{e_2}(x)$ are the parity-check polynomials of two different one-weight irreducible cyclic codes of length $q^k - 1$, whose nonzero weights are, respectively, $q^k - 1$ and $q^{k-1}(q-1)$.
- (B) $\mathcal{C}_{(\Delta e_1, e_2)}$ is an optimal three-weight $[q^k - 1, k+1, q^{k-1}(q-1)-1]$ cyclic code over \mathbb{F}_q , with the weight distribution given in Table I. In addition, if B_j , with $0 < j \leq q^k - 1$, is the number of words of weight j in the dual code of $\mathcal{C}_{(\Delta e_1, e_2)}$, then $B_1 = B_2 = 0$, and

$$B_3 = \frac{(q^k - 3)(q^k - 1)(q - 2)(q - 1)}{6}.$$

Thus, if $q > 2$, then this dual is a single-error-correcting code with parameters $[q^k - 1, q^k - 2 - k, 3]$.

Since the previous reducible cyclic codes are optimal, a natural question that arises is whether there exist other cyclic codes (reducible or irreducible, and apart from those in Theorem 1), whose weight distribution is given in Table I. That is, we ask ourselves if the numerical conditions in Theorem 1, are also necessary. The answer is yes, and we formally state this result in the following:

Theorem 2: Suppose $k > 1$, and let \mathcal{C} be a cyclic code of length $q^k - 1$ over \mathbb{F}_q . Then, the weight distribution of \mathcal{C} is given in Table I if and only if its dimension is $k+1$, and there exist two integers, e_1 and e_2 , in such a way that $h_{\Delta e_1}(x)h_{e_2}(x)$ is the parity-check polynomial of \mathcal{C} , and where these integers satisfy the two conditions: $\gcd(q-1, ke_1 - e_2) = 1$ and $\gcd(\Delta, e_2) = 1$.

As can be seen, the previous result is the natural extension of the characterization given in Theorem 5 of [10]. Now, note that the kind of characterizations that are given in terms of a weight distribution table are, in general, very difficult to establish. One of the most relevant efforts in that direction is the work of B. Schmidt and C. White in [6], where simple necessary and sufficient numerical conditions for an irreducible cyclic code to have at most two weights, are presented. As will be clear later, this important work will be essential in order to present a formal proof of the extended characterization in Theorem 2.

This work is organized as follows: In Section II we fix our notation, give some definitions, and establish the main assumption that must be considered throughout this work. In addition, we recall a characterization about the one-weight irreducible cyclic codes that will be useful. Section III is devoted to recalling the Griesmer lower bound, and also to presenting three preliminary results. In Section IV we study a kind of exponential sums that help us to determine the weights, and their corresponding frequencies, of the codes in Theorem 1. In fact, we are going to present simple necessary and sufficient numerical conditions in order that the evaluation of an exponential sum of such kind is exactly equal to one. In Section V we use the definitions and results of the previous sections in order to present a formal proof of the Theorems 1 and 2. After this, we will analyze the two easy-to-check necessary and sufficient numerical conditions of

Theorem 2 in order to give an explicit formula for the number of cyclic codes that satisfy such conditions. In addition we include, at the end of this section, some examples of Theorems 1 and 2, as well as for such explicit formula. Finally, Section VI is devoted to presenting our conclusions.

II. NOTATION, DEFINITIONS, MAIN ASSUMPTION, AND AN ALREADY-KNOWN RESULT

First of all we set for this section and the rest of this work, the following:

Notation. By using q , k , Δ , e_1 and e_2 , we will denote five integers such that q is the power of a prime number, k is a positive integer, and $\Delta = (q^k - 1)/(q - 1)$. From now on, γ will denote a fixed primitive element of \mathbb{F}_{q^k} . For any integer a , the polynomial $h_a(x) \in \mathbb{F}_q[x]$ will denote the minimal polynomial of γ^{-a} . Furthermore, we will denote by “ $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ ” the trace mapping from \mathbb{F}_{q^k} to \mathbb{F}_q . Lastly, by using χ' and χ we will denote, respectively, the canonical additive characters of \mathbb{F}_{q^k} and \mathbb{F}_q .

A common integer operator in programming languages is the remainder, or modulus operator. This operator is commonly denoted as “%”, and it is interesting to note that it is rarely used in mathematics, and this is so because the remainder of a division of two integers is commonly handled by means of the usual congruence relation among integer numbers. However, as we will see, this remainder operator will be especially important for this work, and therefore a formal definition of it is needed.

Definition 1: Let A and B be two integers such that $B > 0$. Then, $A \% B$ (we read it as the *remainder of A modulus B*), will represent the unique integer r such that $0 \leq r < B$, and $r \equiv A \pmod{B}$.

As examples of the previous definition we have $9 \% 7 = 2$ and $(-9) \% 7 = 5$.

We, now set for this section and the rest of this work, the following:

Main assumption. From now on, we are going to suppose that $\gcd(\Delta, e_2) = 1$ (unless otherwise stated, e_1 is just any integer). Therefore, throughout all this work, we are going to reserve the Greek letters α and β to represent any two integers such that $0 \leq \alpha < q^k - 1$, $0 \leq \beta < q - 1$, and $e_2\alpha + \Delta\beta \equiv 1 \pmod{q^k - 1}$. In order to see that such pair of integers exists, assume that S and T are integers such that $e_2S + \Delta T = 1$. Then, we just need to take $\alpha = S \% (q^k - 1)$ and $\beta = T \% (q - 1)$.

An important type of irreducible cyclic codes are the so-called one-weight irreducible cyclic codes. The following is a characterization for them (see, for example, Theorem 2 in [9]):

Theorem 3: Let a be any integer, and let k' , u , and n be positive integers so that $u = \gcd(\frac{q^{k'} - 1}{q - 1}, a)$, $\frac{q^{k'} - 1}{\gcd(q^{k'} - 1, a)} \mid n$, and $\deg(h_a(x)) = k'$. Then, $h_a(x)$ is the parity-check polynomial of an $[n, k']$ one-weight irreducible cyclic code over \mathbb{F}_q , whose nonzero weight is $\frac{n(q-1)}{q^{k'} - 1} q^{k' - 1}$ if and only if $u = 1$.

III. THE GRIESMER LOWER BOUND AND SOME PRELIMINARY RESULTS

Let $n_q(k, d)$ be the minimum length n for which an $[n, k, d]$ linear code, over \mathbb{F}_q , exists. Given the values of q , k and d , a central problem of coding theory is to determine the actual value of $n_q(k, d)$. A well-known lower bound (see [2] and [7]) for $n_q(k, d)$ is

Theorem 4: (Griesmer bound) With the previous notation,

$$n_q(k, d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

With the aid of the previous lower bound, we now present the following:

Lemma 1: Suppose that \mathcal{C} is a $[q^k - 1, k + 1, q^{k-1}(q - 1) - 1]$ linear code over \mathbb{F}_q . Then \mathcal{C} is an optimal linear code in the sense that its length reaches the lower bound in the previous theorem.

Proof: By means of a direct application of the Griesmer lower bound, we have

$$\begin{aligned} & \left\lceil \frac{q^{k-1}(q-1)-1}{q^0} \right\rceil + \left\lceil \frac{q^{k-1}(q-1)-1}{q} \right\rceil + \cdots + \left\lceil \frac{q^{k-1}(q-1)-1}{q^k} \right\rceil \\ &= [q^{k-1}(q-1)-1] + [q^{k-2}(q-1)] + \cdots + [q-1] + 1 = \Delta(q-1) = q^k - 1. \end{aligned}$$

■

The following two results will be important in order to prove the characterization in Theorem 2.

Lemma 2: Let \mathcal{C} be a cyclic code of length n , over \mathbb{F}_q , with parity-check polynomial $h(x)$. Suppose that \mathcal{C} has exactly $q - 1$ codewords of Hamming weight n . Then, there exists a unique polynomial $h'(x)$, of degree one, such that $h'(x)|h(x)$.

Proof: Let $\mathcal{M} = \{\vec{c} \in \mathcal{C} \mid w_H(\vec{c}) = n\}$, where $w_H(\cdot)$ stands for the usual Hamming weight function. Also let $\sigma : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ be the *circular shift* function defined by $\sigma(x_1, x_2, \dots, x_n) = (x_2, \dots, x_n, x_1)$, for all $(x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$. Now, let $\vec{m} = (m_1, m_2, \dots, m_n)$ be a fixed element of \mathcal{M} . Since, $w_H(\lambda \vec{m}) = n$, for all $\lambda \in \mathbb{F}_q^*$, we can assume, without loss of generality, that $\vec{m} = (m_1 = 1, m_2, \dots, m_n)$. Thus,

$$\mathcal{M} \ni \sigma(\vec{m}) = (m_2, \dots, m_n, m_1) = (m_2 m_1, m_2 m_2, \dots, m_2 m_n) = m_2 \vec{m} \in \{\lambda \vec{m} \mid \lambda \in \mathbb{F}_q^*\} = \mathcal{M},$$

therefore, $m_i = m_2^{i-1}$, for $i = 1, 2, \dots, n$, which in turn means that $\mathcal{M} = \{(\lambda m_2^{i-1})_{i=1}^n \mid \lambda \in \mathbb{F}_q^*\}$. That is, $\mathcal{C}' := \mathcal{M} \cup \{\vec{0}\}$ is a cyclic code of length n and dimension one, whose parity-check polynomial, $h'(x)$, is $h'(x) = x - m_2^{-1}$. But $\mathcal{C}' \subseteq \mathcal{C}$, hence $h'(x)|h(x)$.

Now, suppose that there exists another polynomial, $h''(x)$, of degree one, such that $h''(x)|h(x)$, and $h''(x) \neq h'(x)$. Under these circumstances, and thanks to Theorem 3, $h''(x)$ is the parity-check polynomial of another one-weight irreducible cyclic code of length n , and dimension one, whose nonzero weight is n . Therefore, \mathcal{C} must have at least $2(q - 1)$ codewords of Hamming weight n . A contradiction! ■

The following lemma can be seen as an almost direct consequence of the work of Schmidt and White in [6] (see particularly Corollary 3.2 therein, and Theorem 6 in [9]). As will be clear later, this lemma will be one of the main arguments that will make possible to prove our extended characterization.

Lemma 3: Let k' be a divisor k , and for any suitable integer e , let $\mathcal{C}_{(e)}$ be a $[q^k - 1, k']$ two-weight irreducible cyclic code, over \mathbb{F}_q , whose parity check polynomial is $h_e(x)$. Suppose that $q = p^t$, for some integer t , and some prime p . Thus, if w_1 and w_2 are the nonzero weights of $\mathcal{C}_{(e)}$, then $w_1 - w_2 \neq \pm 1$.

Proof: If $k' < k$, then $\frac{q^k - 1}{q^{k'} - 1} > 1$, and since $\frac{q^k - 1}{q^{k'} - 1} | w_i$, for $i = 1, 2$, $w_1 - w_2 \neq \pm 1$. Suppose $k' = k$. Thus, for a positive integer x , let $S_p(x)$ denote the sum of the p -digits of x . Then, since $\mathcal{C}_{(e)}$ is a $[q^k - 1, k]$ two-weight irreducible cyclic code, we have, owing to Theorem 6 in [9], that $w_1 = \frac{q-1}{q}(q^k - r\varepsilon p^{s\theta})$ and $w_2 = \frac{q-1}{q}(q^k + (u - r)\varepsilon p^{s\theta})$, where $u = \gcd(\Delta, e) > 1$, $f := \text{ord}_u(p)$, $kt = fs$, $\varepsilon = \pm 1$,

$$\theta = \frac{1}{p-1} \min \left\{ S_p \left(\frac{j(p^f - 1)}{u} \right) \mid 1 \leq j < u \right\},$$

and r is a positive integer satisfying:

$$\begin{aligned} r &| (u - 1), \\ rp^{s\theta} &\equiv \pm 1 \pmod{u}, \\ r(u - r) &= (u - 1)p^{s(f-2\theta)}. \end{aligned}$$

Thus, we have $w_1 - w_2 = \pm \frac{q-1}{q} u p^{s\theta}$. But $u > 1$, and $\gcd(q, u) = 1$, therefore $w_1 - w_2 \neq \pm 1$. ■

IV. A CLASS OF EXPONENTIAL SUMS

We want to recall that α and β are integers, with $0 \leq \alpha < q^k - 1$ and $0 \leq \beta < q - 1$, such that $e_2 \alpha + \Delta \beta \equiv 1 \pmod{q^k - 1}$ (see Main assumption). Now, let i, j and v be integers such that $0 \leq i < q^k - 1$, $0 \leq j < q - 1$ and $v = (e_2 i + \Delta j) \% (q^k - 1)$. Then, note that the previous equality implies that $e_2 \alpha v + \Delta \beta v \equiv e_2 i + \Delta j \equiv v \pmod{q^k - 1}$, which in turn implies that $\Delta(\beta v - j) \equiv e_2(i - \alpha v) \pmod{q^k - 1}$. But this last congruence has solution if and only if $\Delta | (i - \alpha v)$ (see, for example, Proposition 3.3.1 in [5]), that is, if and only if $i = (\alpha v + \Delta w) \% (q^k - 1)$ and $j = (\beta v - e_2 w) \% (q - 1)$, where $w = (\frac{i - \alpha v}{\Delta}) \% (q - 1)$. Thus, by keeping this in mind, we now present the following:

Lemma 4: Let

$$\mathcal{V} := \{(i, j) \mid 0 \leq i < q^k - 1 \text{ and } 0 \leq j < q - 1\}.$$

Consider the map $\Phi : \mathcal{V} \rightarrow \mathcal{V}$, given by the rule $\Phi(i, j) = (v, w)$, where $v = (e_2 i + \Delta j) \% (q^k - 1)$ and $w = (\frac{i - \alpha v}{\Delta}) \% (q - 1)$. Then Φ is a bijective map over \mathcal{V} .

Proof: Let $(i, j), (i', j') \in \mathcal{V}$ such that $\Phi(i, j) = \Phi(i', j') = (v, w)$. Then, $\frac{i - \alpha v}{\Delta} \equiv \frac{i' - \alpha v}{\Delta} \equiv w \pmod{q - 1}$, or equivalently, $i - \alpha v \equiv i' - \alpha v \equiv \Delta w \pmod{q^k - 1}$. But $0 \leq i, i' < q^k - 1$, therefore $i = i'$. In a similar way, $e_2 i + \Delta j \equiv e_2 i' + \Delta j' \equiv v \pmod{q^k - 1}$. But we already know that $i = i'$, and since $q^k - 1 = \Delta(q - 1)$ and $0 \leq j, j' < q - 1$, we can conclude that $j = j'$. Thus, Φ is injective. Now, for $(v, w) \in \mathcal{V}$ we take $i = (\alpha v + \Delta w) \% (q^k - 1)$ and $j = (\beta v - e_2 w) \% (q - 1)$. For such a choice of the pair (i, j) , we have $(e_2 i + \Delta j) \% (q^k - 1) = (e_2 \alpha v + e_2 \Delta w + \Delta \beta v - \Delta e_2 w) \% (q^k - 1) = ((e_2 \alpha + \Delta \beta) v) \% (q^k - 1) = v$, and $(\frac{i - \alpha v}{\Delta}) \% (q - 1) = (\frac{\alpha v + \Delta w - \alpha v}{\Delta}) \% (q - 1) = w$. Thus, Φ is also surjective, and Φ is a bijective map. ■

Lemma 5: With our notation, let $d := \gcd(q - 1, k e_1 - e_2)$. Thus, if $d > 1$, then

$$\Delta(e_1 \alpha + \beta) \equiv 1 \pmod{d}.$$

Proof: Since $d \mid (q^k - 1)$, $e_2 \alpha + \Delta \beta \equiv 1 \pmod{d}$. On the other hand, since $\Delta \equiv k \pmod{q - 1}$ (see, for example, Remark 3 in [8]), $d = \gcd(q - 1, \Delta e_1 - e_2)$, and consequently $d \mid (\Delta e_1 - e_2) \alpha$. Therefore, $\Delta(e_1 \alpha + \beta) \equiv e_2 \alpha + \Delta \beta \equiv 1 \pmod{d}$. ■

Lemma 6: With the same notation as above, let $(a, b) \in \mathbb{F}_{q^k}^2$. Define:

$$\begin{aligned} f_{a,b,d} : \mathcal{V} &\rightarrow \mathbb{F}_{q^k}, \\ f_{a,b,d}(v, w) &:= a \gamma^{\Delta(e_1 \alpha + \beta)v + \Delta d w} + b \gamma^v. \end{aligned}$$

If $\rho := \frac{\Delta(e_1 \alpha + \beta) - 1}{d}$, then, for any integer r , and for $t = 0, 1, \dots, d - 1$, we have:

$$\gamma^{r\Delta} f_{a,b,d}(v, w) = f_{a,b,d}((v + r\Delta) \% (q^k - 1), (w - r\rho) \% (q - 1)), \quad (1)$$

$$f_{a,b,d}(v, w) = f_{a,b,d}(v, (w + \frac{q-1}{d}t) \% (q - 1)). \quad (2)$$

Proof: The proof is almost direct from the definition of $f_{a,b,d}(v, w)$;

$$\begin{aligned} \gamma^{r\Delta} f_{a,b,d}(v, w) &= a \gamma^{\Delta(e_1 \alpha + \beta)v + d\Delta w + r\Delta} + b \gamma^{v+r\Delta} \\ &= a \gamma^{\Delta(e_1 \alpha + \beta)(v+r\Delta) + d\Delta w + (1 - \Delta(e_1 \alpha + \beta))r\Delta} + b \gamma^{v+r\Delta} \\ &= a \gamma^{\Delta(e_1 \alpha + \beta)(v+r\Delta) + d\Delta(w - r\rho)} + b \gamma^{v+r\Delta} \\ &= f_{a,b,d}((v + r\Delta) \% (q^k - 1), (w - r\rho) \% (q - 1)). \end{aligned}$$

On the other hand,

$$\begin{aligned} f_{a,b,d}(v, (w + \frac{q-1}{d}t) \% (q - 1)) &= a \gamma^{\Delta(e_1 \alpha + \beta)v + d\Delta w + \Delta(q-1)t} + b \gamma^v \\ &= a \gamma^{\Delta(e_1 \alpha + \beta)v + d\Delta w} + b \gamma^v = f_{a,b,d}(v, w). \end{aligned}$$

Remark 1: Through the function $f_{a,b,d}(v, w)$ we induce a disjoint partition of \mathcal{V} , as follows:

$$\begin{aligned} \mathcal{V}_0 &= \{(v, w) \in \mathcal{V} \mid f_{a,b,d}(v, w) = 0\}, \text{ and} \\ \mathcal{V}_{\gamma^i} &= \{(v, w) \in \mathcal{V} \mid f_{a,b,d}(v, w) = \gamma^i\}, \end{aligned}$$

for $i = 0, 1, \dots, q^k - 2$. Clearly, these subsets are disjoint and $\mathcal{V} = \mathcal{V}_0 \cup (\cup_{i=0}^{q^k-2} \mathcal{V}_{\gamma^i})$. In addition, by (1) we have $|\mathcal{V}_{\gamma^{i+r\Delta}}| = |\mathcal{V}_{\gamma^i}|$ for any integer r . On the other hand, by (2) we also have that there must exist q^k non-negative integers, $N, N_0, N_1, \dots, N_{q^k-2}$, such that $|\mathcal{V}_0| = dN$ and $|\mathcal{V}_{\gamma^i}| = dN_i$. By combining $|\mathcal{V}_{\gamma^{i+r\Delta}}| = |\mathcal{V}_{\gamma^i}|$, with $|\mathcal{V}_{\gamma^i}| = dN_i$, we get $N_{(i+r\Delta)\%(q^k-1)} = N_{i\%(q^k-1)}$, for all integers i and r .

The following result is a generalization of the characterization given in Lemma 3 of [10], that shows that Lemma 6, in [3, p. 4503], can be upgraded to a characterization. Now, note that an interesting feature of the following result is that its proof relies completely on the remainder operator, and on the previous three lemmas, which, by the way, are also based on such operator. Therefore, as we will see next, thanks to this feature we are able to present a simplified and self-contained proof of this generalized characterization.

Lemma 7: Let $(a, b) \in \mathbb{F}_{q^k}^2$, and suppose $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0$ and $b \neq 0$. Consider the sums of the form:

$$T_{(e_1, e_2)}(a, b) := \sum_{x \in \mathbb{F}_{q^k}^*} \sum_{y \in \mathbb{F}_q^*} \chi'(ax^{\Delta e_1}y + bx^{e_2}y) .$$

Then $\gcd(q-1, ke_1 - e_2) = 1$ if and only if $T_{(e_1, e_2)}(a, b) = 1$.

Proof: Clearly,

$$T_{(e_1, e_2)}(a, b) = \sum_{i=0}^{q^k-2} \sum_{j=0}^{q-2} \chi'(a\gamma^{\Delta e_1 i} \gamma^{\Delta j} + b\gamma^{e_2 i} \gamma^{\Delta j}) ,$$

and owing to Lemma 4, we can apply the variable substitutions $i \mapsto (\alpha v + \Delta w)\%(q^k - 1)$, and $j \mapsto (\beta v - e_2 w)\%(q - 1)$ (recall that $e_2 \alpha + \Delta \beta \equiv 1 \pmod{q^k - 1}$). Thus,

$$\begin{aligned} T_{(e_1, e_2)}(a, b) &= \sum_{v=0}^{q^k-2} \sum_{w=0}^{q-2} \chi'(a\gamma^{\Delta(e_1 \alpha + \beta)v} \gamma^{\Delta(\Delta e_1 - e_2)w} + b\gamma^v) \\ &= \sum_{v=0}^{q^k-2} \sum_{w=0}^{q-2} \chi'(a\gamma^{\Delta(e_1 \alpha + \beta)v} \gamma^{\Delta(ke_1 - e_2)w} + b\gamma^v) , \end{aligned} \tag{3}$$

because $\Delta e_1 - e_2 \equiv ke_1 - e_2 \pmod{q-1}$. Now, if $\gcd(q-1, ke_1 - e_2) = 1$, then

$$T_{(e_1, e_2)}(a, b) = \sum_{v=0}^{q^k-2} \sum_{w=0}^{q-2} \chi'(a\gamma^{\Delta w} + b\gamma^v) = \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^k}^*} \chi'(ay + bx) ,$$

and since $b \neq 0$, we have

$$\begin{aligned} T_{(e_1, e_2)}(a, b) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^k} \setminus \{ay\}} \chi'(x) \\ &= \sum_{y \in \mathbb{F}_q^*} \left(\sum_{x \in \mathbb{F}_{q^k}} \chi'(x) - \chi'(ay) \right) \\ &= - \sum_{y \in \mathbb{F}_q^*} \chi'(ay) = - \sum_{y \in \mathbb{F}_q^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a)y) = 1 , \end{aligned}$$

because $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0$.

On the other hand, if $\gcd(q-1, ke_1 - e_2) = d > 1$ then, from (3), we have

$$\begin{aligned}
T_{(e_1, e_2)}(a, b) &= \sum_{v=0}^{q^k-2} \sum_{w=0}^{q-2} \chi'(a\gamma^{\Delta(e_1\alpha+\beta)v}\gamma^{\Delta dw} + b\gamma^v) \\
&= \sum_{v=0}^{q^k-2} \sum_{w=0}^{q-2} \chi'(f_{a,b,d}(v, w)) ,
\end{aligned}$$

where the last equality arises from the definition of the function $f_{a,b,d}(v, w)$ in Lemma 6. Now, by considering the discussion and the notation of Remark 1, we have

$$T_{(e_1, e_2)}(a, b) = |\mathcal{V}_0| \chi'(0) + \sum_{i=0}^{q^k-2} |\mathcal{V}_{\gamma^i}| \chi'(\gamma^i) = d(N + \sum_{i=0}^{q^k-2} N_i \chi'(\gamma^i)) ,$$

however, as was pointed out in Remark 1, $N_{(i+r\Delta)\%(q^k-1)} = N_{i\%(q^k-1)}$ for all integers i and r , therefore,

$$\begin{aligned}
T_{(e_1, e_2)}(a, b) &= dN + d \sum_{i=0}^{\Delta-1} N_i \sum_{r=0}^{q-2} \chi'(\gamma^{i+r\Delta}) \\
&= dN + d \sum_{i=0}^{\Delta-1} N_i \sum_{y \in \mathbb{F}_q^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma^i) y) .
\end{aligned}$$

Now, let $\mathcal{I} = \{0, 1, \dots, \Delta-1\}$, and, by considering the subset $\mathcal{I}_0 = \{i \in \mathcal{I} \mid \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma^i) = 0\}$, we have

$$\begin{aligned}
T_{(e_1, e_2)}(a, b) &= dN + d \sum_{i \in \mathcal{I}_0} (q-1) N_i \chi(0) + d \sum_{i \in \mathcal{I} \setminus \mathcal{I}_0} N_i \sum_{y \in \mathbb{F}_q^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\gamma^i) y) \\
&= d(N + (q-1) \sum_{i \in \mathcal{I}_0} N_i - \sum_{i \in \mathcal{I} \setminus \mathcal{I}_0} N_i) = dt ,
\end{aligned}$$

for some integer t , and since $d > 1$, we have $T_{(e_1, e_2)}(a, b) \neq 1$. ■

We end this section with the following:

Corollary 1: Assume the same notation as before. Thus, if $\gcd(q-1, ke_1 - e_2) = 1$ and $\gcd(\Delta, e_2) = 1$, then

$$T_{(e_1, e_2)}(a, b) = \begin{cases} (q-1)(q^k-1) & \text{if } a = 0 \text{ and } b = 0, \\ -(q^k-1) & \text{if } \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0 \text{ and } b = 0, \\ -(q-1) & \text{if } \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) = 0 \text{ and } b \neq 0, \\ 1 & \text{if } \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0 \text{ and } b \neq 0. \end{cases}$$

Proof: Clearly, $T_{(e_1, e_2)}(0, 0) = (q-1)(q^k-1)$, and if $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0$ and $b = 0$, then

$$\begin{aligned}
T_{(e_1, e_2)}(a, 0) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^k}} \chi'(ax^{\Delta e_1} y) \\
&= \sum_{x \in \mathbb{F}_{q^k}} \sum_{y \in \mathbb{F}_q^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) x^{\Delta e_1} y) = -(q^k-1) .
\end{aligned}$$

On the other hand, if $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) = 0$ and $b \neq 0$, then

$$\begin{aligned}
T_{(e_1, e_2)}(a, b) &= \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^k}^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a)x^{\Delta_{e_1}}y) \chi'(bx^{e_2}y) \\
&= \sum_{x \in \mathbb{F}_{q^k}^*} \sum_{y \in \mathbb{F}_q^*} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(bx^{e_2})y) ,
\end{aligned}$$

but, since $\gcd(\Delta, e_2) = 1$, we have that $|\{x \in \mathbb{F}_{q^k} \mid \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(bx^{e_2}) = 0\}| = q^{k-1}$. Therefore

$$T_{(e_1, e_2)}(a, b) = (q^{k-1} - 1)(q - 1) - q^{k-1}(q - 1) = -(q - 1) .$$

Finally, the proof of the last case comes from the previous lemma. ■

V. FORMAL PROOF OF THEOREMS 1 AND 2

We can now present a formal proof of Theorem 1.

Proof: Part (A): Since $\Delta_{e_1}q \equiv \Delta_{e_1} \pmod{q^k - 1}$, $\deg(h_{\Delta_{e_1}}(x)) = 1$. Let l be the smallest positive integer such that $e_2q^l \equiv e_2 \pmod{q^k - 1}$. Thus $\Delta|e_2\frac{q^l-1}{q-1}$. But $\gcd(\Delta, e_2) = 1$, therefore $(q^k - 1)|(q^l - 1)$, which in turn implies that $\deg(h_{\Delta_{e_1}}(x)) = l = k$. Now, owing to Theorem 3, we know that $\mathcal{C}_{(\Delta_{e_1})}$ is a one-weight irreducible cyclic code, whose nonzero weight is $q^k - 1$. On the other hand, because $\gcd(\Delta, e_2) = 1$, we can conclude, in a similar manner, that $h_{e_2}(x)$ is the parity-check polynomial of a one-weight cyclic code of length $q^k - 1$, whose nonzero weight is $q^{k-1}(q - 1)$.

Part (B): $\mathcal{C}_{(\Delta_{e_1}, e_2)}$ is a $[q^k - 1, k + 1]$ cyclic code due to Part (A). Let \mathcal{A} be a fixed subset of $\mathbb{F}_{q^k}^*$ so that $\{\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \mid a \in \mathcal{A}\} = \mathbb{F}_q^*$. Now, for each $a \in \mathcal{A} \cup \{0\}$ and $b \in \mathbb{F}_{q^k}$, we define $c(q^k - 1, e_1, e_2, a, b)$ as the vector of length $q^k - 1$ over \mathbb{F}_q , which is given by:

$$(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a(\gamma^{\Delta_{e_1}})^i + b(\gamma^{e_2})^i))_{i=0}^{q^k-2} .$$

Thanks to Delsarte's Theorem (see, for example, [1]) it is well known that

$$\mathcal{C}_{(\Delta_{e_1}, e_2)} = \{c(q^k - 1, e_1, e_2, a, b) \mid a \in \mathcal{A} \cup \{0\}, \text{ and } b \in \mathbb{F}_{q^k}\} .$$

Thus the Hamming weight of any codeword $c(q^k - 1, e_1, e_2, a, b)$, will be equal to $q^k - 1 - Z(a, b)$, where $Z(a, b) = \#\{i \mid \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a\gamma^{\Delta_{e_1}i} + b\gamma^{e_2i}) = 0, 0 \leq i < q^k - 1\}$. That is, we have

$$\begin{aligned}
Z(a, b) &= \frac{1}{q} \sum_{i=0}^{q^k-2} \sum_{y \in \mathbb{F}_q} \chi(\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}((a\gamma^{\Delta_{e_1}i} + b\gamma^{e_2i})y)) \\
&= \frac{q^k - 1}{q} + \frac{1}{q} \sum_{y \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^k}^*} \chi'(ax^{\Delta_{e_1}}y + bx^{e_2}y) ,
\end{aligned}$$

and, by using the notation of Lemma 7, we have

$$Z(a, b) = \frac{q^k - 1}{q} + \frac{1}{q} T_{(e_1, e_2)}(a, b) . \tag{4}$$

But $\gcd(q - 1, ke_1 - e_2) = 1$ and $\gcd(\Delta, e_2) = 1$; therefore, after applying Corollary 1, we get

$$Z(a, b) = \begin{cases} q^k - 1 & \text{if } a = 0 \text{ and } b = 0, \\ 0 & \text{if } a \in \mathcal{A} \text{ and } b = 0, \\ q - 1 & \text{if } a = 0 \text{ and } b \neq 0, \\ q & \text{if } a \in \mathcal{A} \text{ and } b \neq 0. \end{cases}$$

Consequently, the assertion about the weight distribution of $\mathcal{C}_{(\Delta e_1, e_2)}$ comes now from the fact that the Hamming weight of any codeword in $\mathcal{C}_{(\Delta e_1, e_2)}$ is equal to $q^k - 1 - Z(a, b)$, and also due to the fact that $|\mathcal{A}| = q - 1$ and $|\mathbb{F}_{q^k}^*| = q^k - 1$.

Lastly, $\mathcal{C}_{(\Delta e_1, e_2)}$ is an optimal cyclic code, due to Lemma 1, and the assertion about the weights of the dual code of $\mathcal{C}_{(\Delta e_1, e_2)}$ can now be proved by means of Table I and the first four identities of Pless (see, for example, pp. 259-260 in [4]). ■

We continue by presenting now a formal proof of Theorem 2.

Proof: Suppose that \mathcal{C} is a cyclic code of length $q^k - 1$, over \mathbb{F}_q , whose weight distribution is given in Table I. Through the sum of the frequencies of such table, it is easy to see that \mathcal{C} must be a cyclic code of dimension $k + 1$. Consequently, the degree of the parity-check polynomial $h(x)$, of \mathcal{C} , must be equal to $k + 1$. Now, note that for any integer e we have that $\deg(h_{\Delta e}(x)) = 1$, therefore, thanks to Lemma 2, there must exist an integer e_1 such that $h_{\Delta e_1}(x) | h(x)$. Let $h'(x) \neq 1$ be an irreducible divisor of $h(x)/h_{\Delta e_1}(x)$, thus, if $k' = \deg(h'(x))$, then $k' > 1$ (owing to Lemma 2), and $k' | k$. Also, let \mathcal{C}' be the irreducible cyclic code of length $q^{k'} - 1$, over \mathbb{F}_q , whose parity-check polynomial is $h'(x)$. Since $\mathcal{C}' \subsetneq \mathcal{C}$, the cyclic code \mathcal{C}' has at most two nonzero weights, and, in accordance with Table I, these nonzero weights may only be $w_1 := q^{k-1}(q - 1) - 1$ and $w_2 := q^{k-1}(q - 1)$. Thus, owing to Lemma 3, and since $w_1 - w_2 = -1$, \mathcal{C}' cannot be a two-weight irreducible cyclic code. Suppose then that \mathcal{C}' is a one-weight irreducible cyclic code of length $q^{k'} - 1$. Now, by further supposing that $k' < k$, we obtain, thanks to Theorem 3, that the nonzero weight of \mathcal{C}' is $\frac{q^{k'} - 1}{q^{k'} - 1}(q - 1)q^{k'-1} > (q - 1)q^{k-1}$. Therefore, this nonzero weight cannot be equal to either w_1 or w_2 . In consequence, $h'(x) = h(x)/h_{\Delta e_1}(x)$ is the parity-check polynomial of a $[q^k - 1, k]$ one-weight irreducible cyclic code, whose nonzero weight is $q^{k-1}(q - 1)$. But by considering again Theorem 3, the previous fact implies that there must exist an integer e_2 such that $\gcd(\Delta, e_2) = 1$, and $h(x) = h_{\Delta e_1}(x)h_{e_2}(x)$.

It remains to prove that $\gcd(q - 1, ke_1 - e_2) = 1$. Let $\mathcal{C}_{(\Delta e_1)}$ and $\mathcal{C}_{(e_2)}$ be the irreducible cyclic codes of length $q^k - 1$ over \mathbb{F}_q , whose parity-check polynomials are, respectively, $h_{\Delta e_1}(x)$ and $h_{e_2}(x)$. If $\gcd(\Delta, e_2) = 1$, then, once again, $\mathcal{C}_{(e_2)}$ will correspond to a one-weight irreducible cyclic code of length $q^k - 1$ and dimension k , whose nonzero weight is $q^k(q - 1)$. Since, in Table I, the frequency of such nonzero weight is $q^k - 1 = |\mathbb{F}_{q^k}^*|$ we have that a codeword c , in \mathcal{C} , will have Hamming weight $q^k(q - 1) - 1$ if and only if $c = c_1 + c_2$, where c_1 and c_2 are, respectively, two nonzero codewords in $\mathcal{C}_{(\Delta e_1)}$ and $\mathcal{C}_{(e_2)}$. But if c_1 and c_2 are nonzero codewords in $\mathcal{C}_{(\Delta e_1)}$ and $\mathcal{C}_{(e_2)}$, then there must exist two finite field elements a and b in \mathbb{F}_{q^k} , with $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \neq 0$, $b \neq 0$, so that the number of zero entries, $Z(a, b)$, in codeword c , can be computed by means of (4). Under these circumstances, codeword c will have Hamming weight $q^k(q - 1) - 1$ if and only if $T_{(e_1, e_2)}(a, b) = 1$, and due to Lemma 7, this can only be possible if and only if $\gcd(q - 1, ke_1 - e_2) = 1$.

Finally, the proof of the converse is just a part of the proof of Theorem 1 that was already given. ■

Due to the simplicity of the necessary and sufficient numerical conditions in Theorem 2, it is possible to compute the total number of different cyclic codes, over \mathbb{F}_q , of length $q^k - 1$ and dimension k , that satisfy such conditions. The following result goes in that direction.

Theorem 5: With our notation, let \mathcal{N} be the number of different cyclic codes, $\mathcal{C}_{(\Delta e_1, e_2)}$, of length $q^k - 1$ and dimension $k + 1$ that satisfy conditions in Theorem 2. Then

$$\mathcal{N} = \frac{\phi(q^k - 1)(q - 1)}{k}, \quad (5)$$

where ϕ denotes the Euler ϕ -function.

Proof: Since $\deg(h_{e_2}(x)) = k$, the total number, \mathcal{N}_2 , of different minimal polynomials $h_{e_2}(x)$ that satisfy condition $\gcd(\Delta, e_2) = 1$ is $\mathcal{N}_2 = \frac{\phi(\Delta)(q-1)}{k}$. On the other hand, since $\deg(h_{\Delta e_1}(x)) = 1$ we have that for each integer e_2 that satisfies $\gcd(\Delta, e_2) = 1$, the total number, \mathcal{N}_1 , of different minimal polynomials $h_{\Delta e_1}(x)$ that satisfy condition $\gcd(q - 1, ke_1 - e_2) = 1$ is $\mathcal{N}_1 = \phi(q - 1) \frac{d}{\phi(d)}$, where $d = \gcd(k, q - 1)$. Now, recall that for any two positive integers m and n , we have $\phi(mn) = \phi(m)\phi(n) \frac{\delta}{\phi(\delta)}$, where $\delta = \gcd(m, n)$.

Thus, $\phi(q^k - 1) = \phi(\Delta(q - 1)) = \phi(\Delta)\phi(q - 1)\frac{d'}{\phi(d')}$, where $d' = \gcd(\Delta, q - 1)$. In consequence, the result follows from the fact that $\mathcal{N} = \mathcal{N}_1\mathcal{N}_2$ and $d' = d$. ■

As a direct consequence of the previous theorem and Theorems 2, we have the following:

Corollary 2: Let \mathcal{N} be the number of different cyclic codes of length $q^k - 1$, over \mathbb{F}_q , whose weight distribution is given in Table I. Then \mathcal{N} is given by (5).

The following are examples related to Theorems 1 and 2, and Corollary 2.

Example 1: With our notation, let $q = 4$, $k = 3$, $e_1 = 2$ and $e_2 = 5$. Then $\Delta = 21$, $\gcd(21, e_2) = 1$ and $\gcd(q - 1, 3e_1 - e_2) = 1$. Therefore, by Theorem 1, we can be sure that $\mathcal{C}_{(42,5)}$ is an optimal three-weight cyclic code over \mathbb{F}_4 , of length 63, dimension 4 and weight enumerator polynomial: $1 + 189z^{47} + 63z^{48} + 3z^{63}$. In addition, $B_1 = B_2 = 0$, and $B_3 = 3843$. In fact, the dual code of $\mathcal{C}_{(42,5)}$ is a $[63, 59, 3]$ cyclic code over \mathbb{F}_4 which, by the way, has the same parameters as the best known linear code, according to the tables of the best known linear codes maintained by Markus Grassl at <http://www.codetables.de/>.

Example 2: With our notation, let $q = 3$ and $k = 4$. Then, owing to Corollary 2, the total number of different cyclic codes of length 80, over \mathbb{F}_3 , and dimension 5, with weight enumerator polynomial $1 + 160z^{53} + 80z^{54} + 2z^{80}$, is $\mathcal{N} = 16$. In fact, these cyclic codes are: $\mathcal{C}_{(0,1)}$, $\mathcal{C}_{(0,7)}$, $\mathcal{C}_{(0,11)}$, $\mathcal{C}_{(0,13)}$, $\mathcal{C}_{(0,17)}$, $\mathcal{C}_{(0,23)}$, $\mathcal{C}_{(0,41)}$, $\mathcal{C}_{(0,53)}$, $\mathcal{C}_{(40,1)}$, $\mathcal{C}_{(40,7)}$, $\mathcal{C}_{(40,11)}$, $\mathcal{C}_{(40,13)}$, $\mathcal{C}_{(40,17)}$, $\mathcal{C}_{(40,23)}$, $\mathcal{C}_{(40,41)}$, and $\mathcal{C}_{(40,53)}$.

VI. CONCLUSIONS

As we already mentioned, in coding theory the weight distribution problem of a cyclic code is an important issue. However, most of the conventional methods employed for the weight distribution computations require the use of, for example, Gauss and/or Jacobi sums along with very sophisticated –but at the same time complex– theorems (for example the Davenport-Hasse Theorem). In this work we used some new and non-conventional methods in order to extend a characterization for the weight distribution of a class of three-weight cyclic codes of dimension 3, to a characterization for the weight distribution of a class of three-weight cyclic codes of dimension greater than or equal to 3, that includes the first characterized class. More specifically, we used the remainder operator, which is quite common in programming languages, in order to show that the numerical conditions given in Theorem 11 of [3, p. 4505] are also necessary, and as a consequence of this, we were able to upgrade such theorem to an extended characterization (Theorems 1 and 2) that includes the characterization given in [10]. Furthermore, we would like to emphasize that by using the remainder operator, we were also able to present a simplified and self-contained proof of our extended characterization. Finally, we also found the parameters for the dual code of any cyclic code in our extended characterization class, and after the analysis of some examples, it seems that such dual codes always have the same parameters as the best known linear codes.

REFERENCES

- [1] P. Delsarte, On subfield subcodes of Reed-Solomon codes, IEEE Trans. Inf. Theory, IT-21(5) (1975) 575-576.
- [2] J.H. Griesmer, A bound for error correcting codes, IBM J. Res. Dev. 4 (1960) 532-542.
- [3] Z. Heng and Q. Yue, Several Classes of Cyclic Codes With Either Optimal Three Weights or a Few Weights, IEEE Trans. Inf. Theory, vol. 62(8) (2016) 4501-4513.
- [4] W.C. Huffman and V.S. Pless, Fundamental of Error-Correcting Codes, Cambridge Univ. Press, Cambridge, 2003.
- [5] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1982.
- [6] B. Schmidt and C. White, All two-weight irreducible cyclic codes?, Finite Fields and their Appl. 8 (2002) 1-17.
- [7] G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, Inform. and Control 8 (1965) 170-179.
- [8] G. Vega, The Weight Distribution of an Extended Class of Reducible Cyclic Codes, IEEE Trans. Inf. Theory, vol. 58(7) (2012) 4862-4869.
- [9] G. Vega, A critical review and some remarks about one- and two-weight irreducible cyclic codes, Finite Fields Appl. 33 (2015) 1-13.
- [10] G. Vega, A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field, Finite Fields Appl. 42 (2016) 23-38.